Amendments to the Specification:

Please replace the one paragraph beginning on line 12 of page 6 of the specification as originally filed with the following two amended paragraphs:

According to ~~an~~ a first aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, and has the steps in the apparatus of transmitting designation information for designating an access area of the memory device, and transmitting together a processing command for the access area and verification information on the designation information, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification information to verify the designation information using the verification information, and executing the processing command when verification succeeds.

According to the aspect of the invention, by dividing a command for access area designation and a command for security protection area access, and adding verification data to the command for security protection area access, a memory device can verify the identity of a device application having specified the access area, a device application having issued the command for security protection area access, and a device application that holds a verification key shared with a memory card, i.e., having right to access the security protected area. Furthermore, regarding memory access, by using a two-stage command constitution, i.e., a

command for access area designation and a command for security protection area access, while command complexity is avoided by using conventional memory card commands, even with only few command argument, without reducing security, access to the security protected area is enabled.

Please replace the one paragraph beginning on page 6, line 25 of the specification as originally filed with the following two amended paragraphs:

According to ~~another~~ a second aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, and has the steps in the apparatus of sharing with the memory device enabled area information on an access enabled area of the memory device, referring to the enabled area information to transmit designation information for designating an access area of the memory device, and transmitting together a processing command for the access area and verification information on the designation information, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification information to verify the designation information using the verification information, and executing the processing command when verification succeeds.

According to the aspect of the invention, whether access by a security protected area

access command is enabled or disabled can be explicitly set to each area in a security protected area.

Please replace the one paragraph beginning on page 7, line 14 of the specification as filed with the following two amended paragraphs:

According to a ~~further~~ third aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, and has the steps in the apparatus of sharing a verification key with the memory device, transmitting designation information for designating an access area of the memory device, and transmitting together a processing command for the access area and verification data obtained by encrypting verification information on the designation information using the verification key, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification data to verify the designation information using the verification data and the verification key, and executing the processing command when verification succeeds.

According to the aspect of the invention, by updating a verification key where needed, security intensity can be enhanced.

Please replace the one paragraph beginning on page 8, line 2 of the specification as filed with the following two amended paragraphs:

According to a ~~further~~ fourth aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, and has the steps in the apparatus of sharing with the memory device enabled area information on an access enabled area of the memory device, further sharing with the memory device a verification key corresponding to the access enabled area, referring to the enabled area information to transmit designation information for designating an access area of the memory device, and transmitting together a processing command for the access area and verification data obtained by encrypting verification information on the designation information using the verification key, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification data to verify the designation information using the verification data and the verification key, and executing the processing command when verification succeeds.

According to the aspect of the invention, when access is not made to an area where only the device can read and write, access by a security protected area access command can be disabled, and thus security intensity can be enhanced. By updating a verification key where needed, security intensity can be enhanced.

Please replace the one paragraph beginning of page 8, line 21 of the specification as filed with the following two amended paragraphs:

According to a ~~further~~ fifth aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, and has the steps in the apparatus of sharing with the memory device enabled area information on an access enabled area of the memory device using a first processing series command, referring to the enabled area information to transmit designation information for designating an access area of the memory device using a second processing series command, and transmitting together a processing command for the access area and verification information on the designation information using the second processing series command , and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification information to verify the designation information using the verification information, and executing the processing command when verification succeeds.

According to the aspect the invention, sharing of information on an accessible area can be divided by command protocol that is different from a command for access area designation and a command for security protection area access, and thus a memory device can verify the identity of a device application having specified the access area, a device application having

issued the command for security protection area access, and a device application having right to access the security protected area.

Please replace the one paragraph beginning on page 9, line 12 of the specification as filed with the following two amended paragraphs:

According to a ~~further~~ sixth aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, and has the steps in the apparatus of sharing a verification key with the memory device using a first processing series command, transmitting designation information for designating an access area of the memory device using a second processing series command, and transmitting together, using the second processing series command, a processing command for the access area and verification data obtained by encrypting verification information on the designation information using the verification key, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification data to verify the designation information using the verification data and the verification key, and executing the processing command when verification succeeds.

According to the aspect of the invention, a verification key sharing process can be divided by command protocol that is different from a command for security protection area access and

by updating a verification key restricted to that area, security intensity can be more enhanced.

Please replace the one paragraph beginning on page 10, line 3 of the specification as filed with the following two amended paragraphs:

According to a ~~further~~ seventh aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, where the memory device has a first area with tamper resistance restricting access from the apparatus, a second area with non-tamper resistance restricting access from the apparatus, and a third area enabling access from the apparatus, and further has the function of distinguishing between at least a first processing series command that is a processing command for the first area and at least a second processing series command that is a processing command for the third area, and the method has the steps in the apparatus of sharing with the memory device enabled area information on an access enabled area of the memory device using the first processing series command, referring to the enabled area information to transmit designation information for designating an access area of the second area using the second processing series command, and transmitting together a processing command for the access area and verification information on the designation information using the second processing series command , and the steps in the memory device of receiving the designation information, further receiving the processing

command and the verification information to verify the designation information using the verification information, and executing the processing command when verification succeeds.

According to the aspect of the invention, an access-enabling setting that is necessary for access to an area with non-tamper resistance is performed by the discretion of a area with tamper-resistance, and read and write of data are performed using commands suitable for the area with non-tamper resistance, whereby both flexibility of security and read and write performance can be achieved.

Please replace the one paragraph beginning on page 11, line 3 of the specification as filed with the following two amended paragraphs:

According to ~~a further~~ an eighth aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, where the memory device has a first area with tamper resistance restricting access from the apparatus, a second area with non-tamper resistance restricting access from the apparatus, and a third area enabling access from the apparatus, and further has the function of distinguishing between at least a first processing series command that is a processing command for the first area and at least a second processing series command that is a processing command for the third area, and the method has the steps in the apparatus of sharing a verification key with the memory device using the

first processing series command, transmitting designation information for designating an access area of the second area using the second processing series command, and transmitting together, using the second processing series command, a processing command for the access area and verification data obtained by encrypting verification information on the designation information using the verification key, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification data to verify the designation information using the verification data and the verification key, and executing the processing command when verification succeeds.

According to the aspect of the invention, an access-enabling setting that is necessary for access to a area with non-tamper resistance and verification key sharing are performed by the discretion of a area with tamper-resistance, and read and write of data are performed using commands suitable for the area with non-tamper resistance, whereby both flexibility of security and read and write performance can be achieved.

Please replace the one paragraph beginning on page 12, line 3 of the specification as filed with the following eight amended paragraphs:

According to a ~~further~~ ninth aspect of the present invention, a memory device is a memory device read or written by an apparatus, and has a processing command receiving

section that receives designation information for designating an area to access, while receiving together verification information based on the designation information and a command for read or write, a designation information verifying section that performs verification processing on the designation information using the verification information, a storage area that stores data, a storage area access section that performs read or write from/in the designated area of the storage area corresponding to the command for processing when the verification processing succeeds, a data transmitting section that transmits data read by the storage area access section to the apparatus, and a data receiving section that receives data to write from the apparatus.

According to the aspect of the invention, even when a command for access area designation is different from a command for accessing a memory, it is possible to verify that the two commands are transmitted from the same terminal.

A tenth aspect of the invention is directed to a memory device such that in the memory device of the ninth invention the verification process of the designation information verifying section is performed using the verification information and a verification key.

According to the aspect of the invention, by using a key, authentication of a terminal using shared secret information with the terminal can be performed.

An eleventh aspect of the invention is directed to a memory device such that the memory device of the tenth invention further comprises verification key sharing section for sharing the verification key with the device.

According to the aspect of the invention, by updating a verification key where needed, security intensity can be enhanced.

A twelfth aspect of the invention is directed to a memory device such that the memory device of the ninth invention further comprises enabled area information sharing section for sharing enabled area information with the device, the enabled area information indicating an area accessible to the memory device.

According to the aspect of the invention, whether access by a security protected area access command is enabled or disabled can be explicitly set to each area in a security protected area.

Please replace the one paragraph beginning on page 12, line 20 of the specification as filed with the following eight amended paragraphs:

According to a ~~further~~ thirteenth aspect of the present invention, an information apparatus is an information apparatus that reads and writes a memory device, and has a designation information determining section which determines an area to read or write, and further determines designation information for designating the area, a verification information generating section that performs processing for generating verification information from the designation information, a processing command transmitting section that transmits the

designation information, while transmitting together the verification information and a processing command for read or write, a data transmitting section that transmits data to the memory device when the processing command is of write, a data receiving section that receives data from the memory device when the processing command is of read, and a data storage section that stores the data to transmit to the memory device, while storing the data received from the memory device.

According to the aspect of the invention, data stored in a security protected area of a memory card can be read and written.

A fourteenth aspect of the invention is directed to an information device such that in the information device of the thirteenth invention the verification information generation process of the Verification information generating section is performed using the specification information and a verification key.

According to the aspect of the invention, by performing verification using a key supplied in secret with a card, data can be stored in an area where read or write cannot be performed by any other device than the information device.

A fifteenth aspect of the invention is directed to an information device such that the information device of the fourteenth invention further comprises a verification key sharing section for sharing the verification key with the memory device.

According to the aspect of the invention, by updating a verification key where needed,

security intensity can be enhanced.

A sixteenth aspect of the invention is directed to an information device such that the information device of the thirteenth invention further comprises an enabled area information sharing section for sharing enabled area information with the memory device, the enabled area information indicating an area accessible to the memory device.

According to the aspect of the invention, when access is not made to an area where only the information device can read and write, access by a security protected area access command can be disabled, and thus security intensity can be enhanced.

Please replace the one paragraph beginning on page 13, line 12 of the specification as filed with the following two amended paragraphs:

According to ~~a further~~ a seventeenth aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, and has the steps in the apparatus of transmitting designation information for designating an access area of the memory device, and transmitting together a processing command for the access area and verification data obtained by encrypting verification information on the designation information using a verification key, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification data to verify the designation information using the verification data and the verification key, and executing the processing

command when verification succeeds.

According to the aspect of the invention, by performing verification using a verification key shared between a device and a memory device, access can be allowed only to the device having right to access.

Please replace the one paragraph beginning on page 13, line 26 of the specification as filed with the following two amended paragraphs:

According to ~~a further~~ an eighteenth aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, and has the steps in the apparatus of sharing enabled area information on an access enabled area of the memory device using a first processing series command, further sharing a verification key corresponding to the access enabled area using the first processing series command, transmitting designation information for designating an access area of the memory device using a second processing series command, and transmitting together, using the second processing series command, a processing command for the access area and verification data obtained by encrypting verification information on the designation information using the verification key, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification data to verify the designation information using the verification

data and the verification key, and executing the processing command when verification succeeds.

According to the aspect of the invention, by validating access by a security protected area access command to an area in a security protected area and updating a verification key limited to that area, security intensity can be more enhanced.

Please replace the one paragraph beginning on page 14, line 19 of the specification as filed with the following four amended paragraphs:

According to a ~~further~~ nineteenth aspect of the present invention, an access method is a method for an apparatus to gain access to a memory device, where the memory device has a first area with tamper resistance restricting access from the apparatus, a second area with a large capacity and non-tamper resistance restricting access from the apparatus, and a third area with a large capacity enabling access from the apparatus, and further has the function of distinguishing between at least a first processing series command that is a processing command for the first area and at least a second processing series command that is a processing command for the third area, and the method has the steps in the apparatus of sharing with the memory device enabled area information on an access enabled area of the memory device using the first processing series command, further sharing a verification key corresponding to the access

enabled area using the first processing series command, transmitting designation information for designating an access area of the second area using the second processing series command, and transmitting together, using the second processing series command, a processing command for the access area and verification data obtained by encrypting verification information on the designation information using the verification key, and the steps in the memory device of receiving the designation information, further receiving the processing command and the verification data to verify the designation information using the verification data and the verification key, and executing the processing command when verification succeeds.

According to the aspect of the invention, an access-enabling setting that is necessary for access to a area with non-tamper resistance and verification key sharing are performed by the discretion of a area with tamper-resistance, and read and write of data are performed using commands suitable for a large capacity area, whereby both flexibility of security and read and write performance can be achieved.

Advantageous Effect of the Invention

According to the present invention, by dividing a command for access area designation and a command for security protection area access, and adding verification data to the command for security protection area access, a card can verify the identity of a terminal application having specified the access area, a terminal application having issued the command for security protection area access, and a terminal application that holds a verification key

shared with the memory card, i.e., having right to access the security protected area. Furthermore, regarding memory access, by using a two-stage command constitution, i.e., a command for access area designation and a command for security protection area access, while command complexity is avoided by using conventional memory card commands, even with only few command argument, without reducing security, access to the security protected area is enabled.

Please insert the following paragraph immediately *before* the paragraph beginning on page 47, line 27 of the specification as filed:

In the present embodiment, a session key sharing step is included in FIG.11. However, if it is considered that there is no need to update a session key each time as security policy, terminal 200 and card 100 may have in advance a verification key and an encryption key and may use the keys as a session key.